

CLAIMS

What is claimed is:

1. A security system for use in a process plant having a process control system that performs product manufacturing related control functions and a safety system that performs safety related control functions with respect to the process plant, comprising:
 - a computer having a processor and a memory;
 - a process controller communicatively coupled to the computer and adapted to perform process control functionality using one or more process control field devices;
 - a safety system controller communicatively coupled to the computer and adapted to perform safety system functionality using one or more safety system field devices;
 - a security database adapted to store access privileges related to both the process control functionality and the safety system functionality;
 - one or more user applications stored in the memory of the computer and adapted to be executed on the processor to communicate process control system messages to or from the process controller and to communicate safety system messages to or from the safety controller; and
 - an integrated security application stored on the memory of the computer and adapted to be executed on the processor to use the security database to enable a user of the one or more user applications to access both the process controller and the safety system controller via the process control system messages and the safety system messages based on access privileges for the user stored in the security database.
2. The security system of claim 1, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity and wherein the user of the one or more user applications is the user entity of at least one of the one or more user accounts.
3. The security system of claim 2, wherein the security database is adapted to store access privileges defining access rights for both the process control system and the safety system based on an identity of a particular user account.

4. The security system of claim 1, wherein the security database is adapted to store access privileges defining access rights for both the process control system and the safety system based on an identity of the computer in which the one or more user applications are executed.

5. The security system of claim 1, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity, wherein the security database is adapted to store access privileges defining access rights for both the process control system and the safety system based on an identity of a particular user account and based on an identity of the computer in which the one or more user applications are executed.

6. The security system of claim 1, wherein at least one of the one or more user applications is a configuration application that enables configuration of both the process controller and the safety system controller.

7. The security system of claim 1, wherein at least one of the one or more user applications is a diagnostics application that enables a user to perform diagnostics with respect to both the process controller and the safety system controller.

8. The security system of claim 1, wherein at least one of the one or more user applications is a viewing application that enables a user to view data with respect to both the process control system and the safety system on a single user display.

9. The security system of claim 8, wherein at least one of the one or more user applications is a write application that enables the user to change parameters within the process control system and the safety system.

10. The security system of claim 9, wherein the security database includes a procedures database that stores a write procedure for implementing a write to the safety system and wherein the security application automatically implements the write procedure when the at least one of the one or more user applications implements a write to the safety system.

11. The security system of claim 10, wherein the write procedure is a repeat write confirmation procedure that sends two write commands to perform a write.

12. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system and wherein the security database is adapted to store a first one of the possible levels of access privileges for a particular user for the process control system and a second and different one of the possible levels of access privileges for the particular user for the safety system.

13. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein a first one of the possible levels of access privileges enables a user to read parameters from the process control system or the safety system and a second one of the possible levels of access privileges enables a user to write parameters to the process control system or to the safety system.

14. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein one of the possible levels of access privileges enables a user to create logic to be implemented in the process control system or in the safety system.

15. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein one of the possible levels of access privileges enables a user to download logic to be implemented in the process control system or in the safety system to the process controller or to the safety system controller.

16. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein one of the possible levels of access privileges enables a user to write parameters in the process control system or in the safety system.

17. The security system of claim 1, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein one of the possible levels of access privileges enables a user to calibrate a device within the process control system or a device within the safety system.

18. The security system of claim 1, wherein the security database is adapted to store access privileges for each of a multiplicity of different users, wherein an access privilege for a particular user defines a first access privilege for the process control system and a second access privilege for the safety system.

19. The security system of claim 1, wherein the at least one of the one or more user applications is adapted to present a display to a user having a first set of fields related to the process control system and a second set of fields related to the safety system and wherein the security application detects if an operation is being made to the process control system or to the safety system based on an identity of a field of the display.

20. The security system of claim 1, wherein at least one of the one or more user applications is adapted to present a display to a user having a first set of fields related to the process control system and a second set of fields related to the safety system, with each field in the first and the second sets of fields having an associated tag, and wherein the security application detects if an operation is being made to the process control system or to the safety system based on the tag associated with a field of the display.

21. The security system of claim 20, wherein each tag includes a path that defines whether an associated one of the fields is associated with a process control system unit or with a safety system unit.

22. The security system of claim 1, wherein the security application detects if an operation within one of the one or more user applications is being made to a process control system unit or to a safety system unit and applies access privileges as stored in the security database based on whether the operation is being made to a process control system unit or to a safety system unit.

23. The security system of claim 22, wherein the security application stores a security procedure to be implemented based on whether or not the operation is being made to a safety system unit and wherein the security application implements the security procedure when the operation is being made to a safety system unit.

24. A security system for use in a process plant having a process control system that performs product manufacturing related control related functions using one or more process control field devices and a safety system that performs safety related control functions using one or more safety field devices, the security system comprising:

- a computer having a processor and a memory;
- a process controller communicatively coupled to the computer and adapted to perform process control system functionality using the one or more process control field devices;
- a safety system controller communicatively coupled to the computer and adapted to perform safety system functionality using the one or more safety system field devices;
- a security database adapted to store access privileges related to both the process control system functionality and the safety system functionality;
- one or more user applications stored in the memory of the computer and adapted to be executed on the processor to communicate process control system messages to or from the process controller and to communicate safety system messages to or from the safety system controller using a common communication format, wherein each message has a data field indicating whether the message is associated with a process control system entity or a safety system entity; and
- an integrated security application stored on the memory and adapted to be executed on the processor to distinguish whether an operation to be implemented by one of the one or more user applications is related to a process control system entity or to a safety system entity and to use the security database to enable a user of the one of the one or more user applications to perform the operation based on access privileges for the user stored in the security database.

25. The security system of claim 24, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity and wherein the user of the one or more user applications is the user entity of at least one of the one or more user accounts.

26. The security system of claim 24, wherein the data field of each message that indicates whether the message is associated with a process control system entity or a safety system entity is an address field.

27. The security system of claim 24, wherein the data field of each message that indicates whether the message is associated with a process control system entity or a safety system entity is a tag indicating a communication path.

28. The security system of claim 24, wherein the security application distinguishes whether an operation to be implemented by the one of the one or more user applications is related to a process control system entity or to a safety system entity based on the data field within a message associated with the operation.

29. The security system of claim 24, wherein the security database is adapted to store access privileges defining access rights for both the process control system entities and the safety system entities based on an identity of a particular user

30. The security system of claim 29, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity and identity of the particular user is determined as the user entity of at least one of the one or more user accounts.

31. The security system of claim 24, wherein the security database is adapted to store access privileges defining access rights for both the process control system entities and the safety system entities based on an identity of the computer in which the one of the one or more user applications is executed.

32. The security system of claim 24, wherein the security database is adapted to store access privileges defining access rights for both the process control system entities and the safety system entities based on an identity of a particular user and based on an identity of the computer in which the one of the one or more user applications is executed.

33. The security system of claim 24, wherein one of the one or more user applications is a configuration application that enables configuration of both the process control system entities and the safety system entities.

34. The security system of claim 24, wherein one of the one or more user applications is a diagnostics application that enables a user to perform diagnostics with respect to both the process control system entities and the safety system entities.

35. The security system of claim 24, wherein one of the one or more user applications is a write application that enables the user to change parameters within the process control system entities and the safety system entities.

36. The security system of claim 24, wherein the security database includes a procedures database that stores a write procedure for implementing a write to one of the process control system entities and the safety system entities and wherein the security application automatically implements the write procedure when the one of the one or more user applications implements a write to the one of the process control system entities and the safety system entities.

37. The security system of claim 36, wherein the write procedure is a repeat write confirmation procedure that sends two write commands.

38. The security system of claim 24, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity, wherein the security database is also adapted to store a multiplicity of different possible levels of access privileges with respect to each of the process control system and the safety system and wherein the security database is adapted to store a first one of the possible levels of access privileges for a particular user account for the process control system and a second and different one of the possible levels of access privileges for the particular user account for the safety system.

39. The security system of claim 24, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity, and wherein the security database is also adapted to store a multiplicity of different possible levels of access privileges with respect to each of the process control system and the safety system, wherein a first one of the possible levels of access privileges enables a user account to read parameters from the process control system or the safety system and a second one of the possible levels of access privileges enables a user account to write parameters to the process control system or to the safety system.

40. The security system of claim 39, wherein a third one of the possible levels of access privileges enables a user account to create logic to be implemented in the process control system or in the safety system.

41. The security system of claim 40, wherein a fourth one of the possible levels of access privileges enables a user account to download logic to be implemented in the process control system or in the safety system to the process controller or to the safety system controller.

42. The security system of claim 40, wherein a fifth one of the possible levels of access privileges enables a user account to perform a calibration procedure to be implemented in the process control system or in the safety system.

43. The security system of claim 24, wherein the security database is adapted to store access privileges for each of a multiplicity of different users, wherein the access privileges for a particular user defines a first access privilege for the process control system and a second access privilege for the safety system.

44. A security system for use in a process plant having a process control system with a process controller adapted to perform product manufacturing related control functionality using one or more process control field devices, a safety system having a safety system controller adapted to perform safety related control functionality using one or more safety system field devices, and a host computer having a processor communicatively coupled to the process controller and to the safety system controller and one or more user applications executed on the processor to communicate process control system messages to or from the process controller and to communicate safety system messages to or from the safety controller, the security system comprising:

- a memory;

- a security database adapted to store access privileges related to both the process control system and the safety system; and

- a security application stored on the memory and adapted to be executed on the processor to enable the one or more user applications to access the process control system and the safety system via the process control system messages and the safety system messages based the access privileges stored in the security database.

45. The security system of claim 44, wherein the security database stores access privileges for one or more user accounts, wherein each user account includes access privileges for a separate user entity.

46. The security system of claim 44, wherein the security database is adapted to store access privileges defining access rights for both the process control system and the safety system based on an identity of a particular user.

47. The security system of claim 44, wherein the security database is adapted to store access privileges defining access rights for both the process control system and the safety system based on an identity of the computer in which the one or more user applications are executed.

48. The security system of claim 44, wherein the security database includes a procedures database that stores a write procedure for implementing a write to at least one of the process control system and the safety system and wherein the security application automatically implements the write procedure when the one or more user applications implement a write to the one of the process control system and the safety system.

49. The security system of claim 48, wherein the write procedure is a repeat write confirmation procedure the generates two write commands.

50. The security system of claim 44, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system and wherein the security database is adapted to store a first one of the possible levels of access privileges for a particular user for the process control system and a second and different one of the possible levels of access privileges for the particular user for the safety system.

51. The security system of claim 44, wherein the security database is adapted to store a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein a first one of the possible levels of access privileges enables a user to read parameters from the process control system or the safety system and a second one of the possible levels of access privileges enables a user to write parameters to the process control system or to the safety system.

52. The security system of claim 44, wherein the security database is adapted to store access privileges for each of a multiplicity of different user accounts, wherein the access privileges for each particular user account defines a first access privilege for the process control system and a second access privilege for the safety system.

53. The security system of claim 44, wherein the security application is adapted to detect if an operation within the one or more user applications is being made to a process control system unit or to a safety system unit and to apply access privileges as stored in the security database based on whether the operation is being made to a process control system unit or to a safety system unit.

54. A method of performing security procedures in a process plant having a process control system with a process controller adapted to perform product manufacturing control functionality using one or more process control field devices and a safety system having a safety system controller adapted to perform safety related functionality using one or more safety system field devices, the method comprising:

storing access privileges related to both the process control system and the safety system in a security database;

detecting whether an action to be taken with respect to the process plant is an action related to the process control system or to the safety system;

determining an appropriate set of access privileges from the security database based on whether the action to be taken is related to the process control system or to the safety system; and

preventing or allowing the action to be taken based on the appropriate set of access privileges.

55. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes storing access privileges defining access rights for both the process control system and the safety system based on an identity of a particular user entity initiating the action to be taken.

56. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes storing access privileges defining access rights for both the process control system and the safety system based on an identity of a computer initiating the action to be taken.

57. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes storing access privileges defining access rights for both the process control system and the safety system based on an identity of a particular user entity initiating the action to be taken and an identity of a computer initiating the action to be taken.

58. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges includes storing a security procedure for implementation with respect to one of the process control system and the safety system and further including automatically implementing the security procedure when the appropriate set of access privileges allows the action to be taken.

59. The method of performing security procedures in a process plant according to claim 58, wherein the security procedure is a repeat write confirmation procedure and wherein automatically implementing the security procedure includes performing the repeat write confirmation procedure when the action to be taken is a write to one of the process control system or to the safety system.

60. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes defining a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, and including storing a first one of the possible levels of access privileges for a particular user entity for the process control system and a second and different one of the possible levels of access privileges for the particular user entity for the safety system.

61. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes defining a multiplicity of different possible levels of access privileges for each of the process control system and the safety system, wherein a first one of the possible levels of access privileges enables a user entity to read parameters from the process control system or from the safety system and a second one of the possible levels of access privileges enables a user entity to write parameters to the process control system or to the safety system.

62. The method of performing security procedures in a process plant according to claim 61, wherein a third one of the possible levels of access privileges enables a user entity to create logic to be implemented in the process control system or in the safety system.

63. The method of performing security procedures in a process plant according to claim 61, wherein a third one of the possible levels of access privileges enables a user entity to download logic to be implemented in the process control system or in the safety system.

64. The method of performing security procedures in a process plant according to claim 61, wherein a third one of the possible levels of access privileges enables a user entity to perform a calibration procedure in the process control system or in the safety system.

65. The method of performing security procedures in a process plant according to claim 54, wherein storing access privileges in the security database includes storing access privileges for a particular user entity that defines a first access privilege for the process control system and a second access privilege for the safety system.

66. The method of performing security procedures in a process plant according to claim 54, wherein detecting whether an action to be taken with respect to the process plant is an action related to the process control system or to the safety system includes determining whether a field in a message associated with the action to be taken identifies a process control system device or a safety system device.

67. The method of performing security procedures in a process plant according to claim 54, wherein detecting whether an action to be taken with respect to the process plant is an action related to the process control system or to the safety system includes determining whether a field in a user display from which the action is initiated is associated with a process control system parameter or a safety system parameter.